Design of Service Oriented Architecture(SOA)-based Software Vulnerability Analysis Method for Digital I&C System in NPP

J. G. Song [a*], C. K. Lee [a], K. H. Kim [b], K. C. Kwon [a], S. S. Kim [c]
[a] *Korea Atomic Energy Research Institute, I&C & HF Research Div.,*
1045 Daedeok-Daero, Yuseong-gu, Daejeon, 305-353, Republic of KOREA
[b] *Shinsegae Information & Communication Co., Ltd., 197-12, Guro-Dong, Seoul, Republic of KOREA*
[c] *Department of Multimedia, Hannam Univ.,133, Ojeong-dong, Daedeok-gu, Daejeon, Republic of KOREA*
[*] *Corresponding author: jgsong@kaeri.re.kr*

1. Introduction

Diverse cyber security issues due to the vulnerability of the digital control systems have been brought up in the existing IT environments while advancement and propagation of digital I&C systems have improved convenience through automation[1]. The recent example of Stuxnet proved that stability in the digital I&C system could not be secured due to an air gap of physical security elements[2]. Therefore, it is required to discover new approaches toward cyber security that will overcome the limitation on security in a closed environment. In particular, there is a rapid increase in the importance of cyber security seen in guidelines published by IAEA and U.S. NRC shows that cyber security as well as physical security draws worldwide attention as a key component for nuclear system safety[3, 4, 5]. To incorporate the new guide requirement, cyber security threats are analyzed by IT-base security elements for finding best practice approaches. The vulnerabilities identified by the general security threats and defined mitigation activities can include many different methods and strategies. This research suggests a method for analyzing vulnerability and assessment the nuclear digital I&C cyber security.

2. Fundamental Research

The research on vulnerability of cyber security requires measures to implement tools for analyzing vulnerable tools currently in use in order to analyze vulnerability of cyber security.

2.1 Tools for Analyzing Vulnerability

Vulnerability analysis tools identify a system vulnerability that includes threats of illegal user's access to information system, threats of interruption to regular operation and services, important data leak, and modification and deletion and inform responsive solutions to such security vulnerability through the analysis of information system security levels[6].

The first step in the nuclear digital I&C cyber security assessment to implement optimal security technology is analyzing vulnerability of current system. Indiscriminate implementation of IT-based security solutions to the nuclear digital I&C environment is not the only way to improve security. Due to the operational property of I&C in the nuclear power plant that prioritizes usability, implementation of an unnecessary security method can cause overload and affect negatively in usability, which may lead to fatal problems. Therefore, it is critical to analyze various threats to cyber security occurred in existing IT environments and to determine the threatening elements and their impact on the system. In order to resolve such issues, it is required to implement security vulnerability analysis tools and methods that generate objective and relevant data and provide practical guidelines for information system security.

Typical security vulnerability is analyzed on three threats as following:

-Threat that permits illegal access;
-Threat that prevents normal operations and services;
-Threat of data leak, modification and deletion of information.

2.2 Vulnerability Check from IT perspective

Vulnerability checks from IT perspective include:

-Inspection of operation status and system setting of major server equipment;
-Inspection of network vulnerability;
-Inspection of security systems (Firewall, IDS); and
-Inspection of application systems (security of source codes and application system security function).

Most of vulnerability inspections are conducted manually according to a checklist and using self-assessment tools within measurable areas.

2.3 SOA Approach to Security

SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the of different ownership domains. Standardizing technologies used in SOAs increases interoperability[7].

Most existing cyber security solutions simply look for signature-based threats that search for known malicious patterns. SOA is one of best methods in the classification of security categories for analyzing existing attack patterns for each different area of cyber security.

3. SOA-based Analysis method for the assessment of I&C cyber security

To realize the cyber security of digital I&C, it requires the establishment of process where one identifies potential problems by evaluating the threat elements, and then analyze possible solutions and apply them in an appropriate time. The most important step is that it is impossible to take corrective measures if there is no complete understanding and accurate identification of problems.

In light of the above, this research suggests the process for analysis method.

-Analyze IT security cases and techniques

-Design of plans for nuclear digital I&C cyber security

-Development of policies, guideline and checklists

For the analysis of IT security cases and techniques, it requires close examination of attack routes, targets, and vulnerability and after determining whether a nuclear digital I&C system is being threatened, one should classify attack techniques and countermeasures by types.

Then, based on the information at hand and considering the distinctive characteristics of nuclear I&C, one should derive plans for countermeasures for the purpose of managing IT security threats.

Lastly, by matching the policies, procedures, guidelines, and manuals pertaining to nuclear cyber security with IT security cases and techniques, one should develop the countermeasure lists for nuclear I&C cyber security and provide assessment guideline. This plan is developed complying with the specific characteristics of nuclear power plant.

With the cyber security checklist developed though the above process, one can analyze system software designed by a developer and use as a classification standard to identify the characteristics and importance level of each component.

Additionally, with the designed digital I&C cyber security checklist and by comparing and analyzing the cases where existing IT and infrastructure has been threatened, the proposal for optimal security model for nuclear I&C is possible.

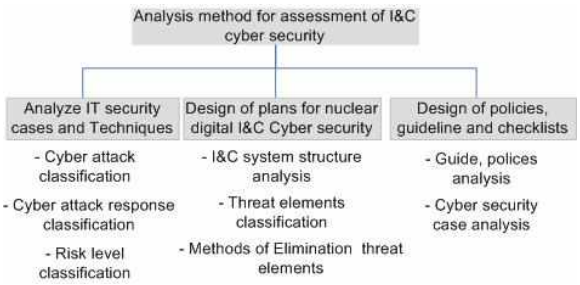

Fig. 1. Domain analysis for Digital I&C cyber security

The above process involves identifying the scenarios for failures and development of checklists to resolve error elements as a result of failures. Additionally, through the guideline of nuclear cyber security, one can infer the precaution matters in developmental phases and essential elements for the purpose of security.

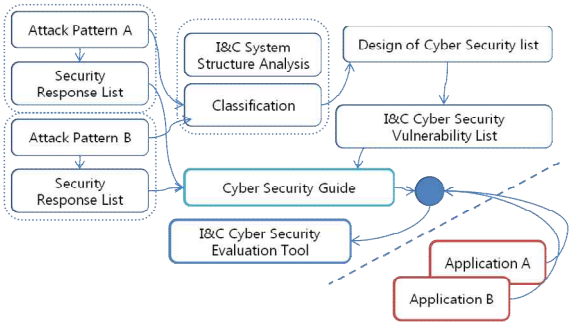

Fig. 2. Analysis using SOA.

4. Conclusions

This research was conducted as the details of cyber security policies, guidelines and scenarios in related to nuclear power plant is not clearly defined and as its scope is broad and extensive there are difficulties in applying to the current system and in developing countermeasures

Based on the problem above, through the analysis of vulnerability of IT security, we conducted analysis of nuclear digital I&C cyber security. This research provides foundation to improve the system through the development of checklist that specifies the current and potential threats and through the application of method that resolves problems, and by giving shape to the regulations on the nuclear cyber security.

Acknowledgement

The work has been performed with the support of the Ministry of Knowledge and Economy since 2010.

REFERENCES

[1] Countering Challenges to the Global Supply Chain, Cyber Threats to National Security, 2010.

[2] Symantec: Win32.Stuxnet Dossier, http://www.symantec.com/connect/blogs/w32stuxnet-dossier.

[3] USNRC Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.

[4] USNRC Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, 2010.

[5] NIST SP 800-82, Guide to Industrial Control Systems Security, 2008.

[6] Oleg Sheyner, JeannetteWing, Tools for Generating and Analyzing Attack Graphs, FMCO 2003, LNCS 3188, pp. 344–371, 2004.

[7] Faouzi Kamoun, A Roadmap towards the Convergence of Business Process Management and Service Oriented Architecture, 2007